

內政部指定營建類非公務機關個人資料檔案安全維護管理辦法總說明

個人資料保護法(以下簡稱本法)第二十七條規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」鑑於加強個人資料保護之需求日益殷切，有必要規範並監督非公務機關訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法，以促使其採取適當措施，降低個人資料損害，並在個人資料蒐集、處理或利用過程中，善盡個人資料保護責任，爰依本法第二十七條第三項規定授權，並參酌本法施行細則第十二條規定，訂定內政部指定營建類非公務機關個人資料檔案安全維護管理辦法（以下簡稱本辦法），共計二十五條，其要點如下：

- 一、本辦法之訂定依據、主管機關、適用範圍。（第一條至第三條）
- 二、非公務機關應訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）、訂定內容及報備查期限。（第四條）
- 三、非公務機關應配置適當管理人員及提供相當資源，以執行本計畫及處理方法，及公告個人資料保護管理政策等事項。（第五條）
- 四、界定個人資料範圍、風險評估、個人資料事故之預防、應變、通報機制。（第六條至第九條）
- 五、個人資料蒐集、處理及利用之內部管理程序。（第十條至第十三條）
- 六、資料安全管理、資通訊系統安全管理、設備安全管理、人員管理、認知宣導及教育訓練。（第十四條至第十八條）
- 七、個人資料安全維護稽核機制；使用紀錄、軌跡資料及證據保存；個人資料安全維護之整體持續改善。（第十九條至第二十一條）
- 八、業務終止後之個人資料處理方法。（第二十三條）
- 九、本辦法施行日期。（第二十五條）

內政部指定營建類非公務機關個人資料檔案安全維護管理辦法

條文	說明
第一條 本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	本辦法訂定依據。
第二條 本辦法所稱主管機關，在中央為內政部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。	本辦法主管機關。
第三條 本辦法所稱非公務機關，包括下列各款： 一、營造業。 二、不動產開發業。 三、建築師事務所。 四、公寓大廈管理維護公司。 五、都市更新業務財團法人。 六、其他經中央主管機關公告指定者。 前項第二款不動產開發業，指以銷售為目的，從事土地、建物等不動產投資興建之行業。	一、第一項定明本辦法之適用對象為：營造業（包括綜合營造業、專業營造業、土木包工業）、不動產開發業、建築師事務所、公寓大廈管理維護公司及都市更新業務財團法人；另為因應日後可能納入管理之非公務機關需求，於第六款規定其他經中央主管機關公告指定者。 二、第二項定明第一項第二款之不動產開發業範疇。不動產開發業對應之營業項目為住宅及大樓開發租售業、工業廠房開發租售業、特定專業區開發業、投資興建公共建設業、新市鎮、新社區開發業、區段徵收及市地重劃代辦業、都市更新重建業或都市更新整建維護業。其中住宅及大樓開發租售業、工業廠房開發租售業者倘僅經營不動產租售業務，未涉及不動產開發業務者，非屬不動產開發業。
第四條 非公務機關應訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法），以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 非公務機關依前項規定訂定本計畫及處理方法時，應視其業務規模、特性、保有個人資料之性質及數量等事項，參酌第五條至第二十三條規定，訂定包含下列各款事項之適當安全維護管理措施；必要時，第二款各目事項得整併之： 一、非公務機關之組織規模及特性。 二、個人資料檔案之安全管理措施： （一）配置管理之人員及相當資源。 （二）界定蒐集、處理及利用個人資	一、第一項及第二項定明非公務機關訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）之義務及訂定內容。 二、非公務機關訂定本計畫及處理方法，應於一定期限內報請主管機關備查，爰為第三項及第四項規定。

料之範圍。 (三) 個人資料之風險評估及管理機制。 (四) 事故之預防、通報及應變機制。 (五) 個人資料蒐集、處理及利用之內部管理程序。 (六) 設備安全管理、資料安全管理及人員管理措施。 (七) 認知宣導及教育訓練。 (八) 個人資料安全維護稽核機制。 (九) 使用紀錄、軌跡資料及證據保存。 (十) 個人資料安全維護之整體持續改善。 (十一) 業務終止後之個人資料處理方法。 第一項之本計畫及處理方法，都市更新業務財團法人應於主管機關許可設立之日起六個月內報請其主管機關備查，其餘非公務機關應於開業或完成營業項目登記之日起六個月內，報請主事務所所在地之直轄市、縣（市）主管機關備查。 中央主管機關依前條第一項第六款公告指定前，已完成開業、營業項目登記或財團法人許可設立者，應於公告指定之日起六個月內，將第一項之本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。	
第五條 非公務機關應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行本計畫及處理方法等相關事項，並定期向負責人提出報告。 非公務機關應訂定個人資料保護管理政策，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於營業處所或主事務所適當之處；如有網站者，並揭露於網站首頁，使其所屬人員及個人資料當事人均能知悉。	一、為有效訂定與執行本計畫及處理方法等相關個人資料保護事項，非公務機關應先進行組織任務分工，配置適當之管理人員及資源，就本計畫及處理方法相關事項，作相關程序之規劃、訂定、修正及執行，並定期報告計畫推動情形，爰為第一項規定。 二、第二項規定非公務機關應訂定個人資料保護管理政策並公告，使其所屬人員及個人資料當事人均能知悉。
第六條 非公務機關應界定納入本計畫及處理方法之個人資料範圍，辦理下列事項： 一、定期清查保有之個人資料現況。 二、確認保有之個人資料所應遵循適	一、個人資料通常分散於不同部門及地點，為瞭解保有及管理個人資料，非公務機關應定期進行個人資料清查，界定其保有及管理個人資料項目之內涵（個人資料檔案名稱、特定目的、個

用之個人資料保護相關法令現況。	人資料類別、保有個人資料之法令依據及保有單位等），並以書面或網頁說明等方式具體說明特定目的項目及代號，俾利有效規劃個人資料保護事項並落實各管理措施。清查依個人資料生命週期及資料流程，先檢視有無個人資料保護法（以下簡稱本法）第五十一條規定排除個人資料類型，再鑑別個人資料類型如員工、客戶，爰為第一款規定。 二、為瞭解保有及管理個人資料是否合法，應確認所適用個人資料保護之相關法令現況，例如人事差勤系統，其保有依據為勞動基準法，應清查該法令適用個人資料保護之現況，爰為第二款規定。
第七條 非公務機關應依前條已界定之個人資料範圍及蒐集、處理、利用個人資料之流程，評估可能產生之風險，並根據風險評估之結果，依風險等級訂定適當之管控措施。	非公務機關依前條個人資料清查結果，建立風險評估或隱私權衝擊分析之標準，針對風險，採取適當之解決對策或控制措施，以有效降低個人資料檔案遭受損害之風險。
第八條 非公務機關為因應保有之個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱個人資料事故），應採取下列應變、通報及預防機制： 一、採取適當之應變措施，以控制個人資料事故對當事人之損害，並通報內部有關單位。 二、查明個人資料事故之狀況並以適當方式通知當事人有關個人資料事故事實、所為因應措施及諮詢服務專線等內容。 三、研議預防機制，避免類似個人資料事故再次發生。	非公務機關應依據前條個人資料風險評估結果，訂定個人資料事故之預防、通報及應變程序，以強化事前預防避免、事中應變通報、事後檢討改進之機制，爰為第一款至第三款規定如下： 一、通報區分一般及重大個人資料事故。第一款為一般個人資料事故，屬非公務機關能自行掌控處理之事件，依內部程序通報有關單位；第九條為重大個人資料事故，應依內部程序通報有關單位，並依外部程序於時限內通報主管機關。 二、依本法第十二條規定，個人資料被竊取、洩漏、竄改或其他侵害，非公務機關應查明後以適當方式通知當事人；本法施行細則第二十二條業規定適當之通知方式，且通知內容應包括個人資料被侵害之事實及已採取之因應措施；另非公務機關應提供諮詢服務專線供當事人諮詢，使當事人知悉個人資料遭違法侵害情事，及時採取補救措施或提起救濟，以降低損害之擴大。 三、依據已發生之個人資料事故，重新審視風險評估或隱私權衝擊分析之標準，研擬預防機制，防止類似個人資料

	事故再度發生，並確認預防措施之有效性。
第九條 非公務機關依前條第一款通報者為重大個人資料事故，應於發現後七十二小時內，將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現事故後立即通報等事項，以書面通報主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關；如為直轄市、縣（市）主管機關接獲通報，並應副知中央主管機關（書面通報格式如附件）。 前項所稱重大個人資料事故，指個人資料被竊取、竄改、毀損、滅失或洩漏達一千筆以上，將危及非公務機關正常營運或大量當事人權益之情形。 主管機關接獲通報或主動知悉事故，得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。	一、第一項定明非公務機關遇有重大個人資料事故時，負通報義務，並依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，定明事故通報之對象、時點及應通報事項。 二、參考製造業及技術服務業個人資料檔案安全維護管理辦法第二條規定及考量所納管個人資料之重要性，爰第二項定明非公務機關遇有達一千筆以上個人資料被竊取、竄改、毀損、滅失或洩漏為重大個人資料事故，以區別一般及重大個人資料事故。 三、為調查事故發生後，是否係非公務機關所採取保護安全措施不足導致，第三項定明主管機關得採取之措施及後續行政檢查規定。
第十條 非公務機關所屬人員對於個人資料蒐集、處理及利用，應注意下列事項： 一、屬本法第六條所定特種個人資料者，應檢視其特定目的及是否符合相關法令之要件；其經當事人書面同意者，應符合本法第七條第一項、第二項及第四項規定。 二、檢視一般個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定要件。其經當事人同意者，應符合本法第七條第一項、第三項及第四項規定。 三、檢視一般個人資料之利用，是否符合本法第二十條規定，於蒐集之特定目的必要範圍內為之；特定目的外之利用，是否符合本法第二十條第一項但書規定。其經當事人同意者，應符合本法第七條第二項及第四項規定。 四、利用個人資料為行銷，當事人表示拒絕行銷後，立即停止利用其	一、依本法第六條立法目的，病歷、醫療、基因、性生活、健康檢查及犯罪前科六項特種個人資料，有特別加強保護之必要，除符合該條第一項但書所定六款例外情形外，原則上不得蒐集、處理或利用。其經當事人書面同意者，應符合本法第七條規定，爰為第一款規定。 二、本法第十九條第一項規定，非公務機關蒐集或處理一般個人資料，應具備特定目的且符合該條第一項所定八款法定情形之一。其經當事人同意者，應符合本法第七條規定，爰為第二款規定。 三、本法第二十條第一項規定，非公務機關對於一般個人資料之利用，應於蒐集之特定目的必要範圍內為之，具備該條第一項但書所定七款法定情形之一者，得為特定目的外之利用。其經當事人同意者，應符合本法第七條規定，爰為第三款規定。 四、依本法第二十條第二項及第三項規定，非公務機關利用個人資料行銷，於

個人資料行銷，且周知所屬人員，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。 五、於蒐集、處理或利用過程中，檢視個人資料是否正確，有不正確時，應主動更正或補充。其正確性有爭議者，應依本法第十一條第二項規定辦理。	首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。當事人表示拒絕接受行銷時，非公務機關應即停止利用其個人資料行銷，爰為第四款規定。 五、個人資料之正確性，攸關能有效利用個人資料以提供當事人相關服務，爰於作業程序上應檢視個人資料是否正確，並適時更正或補充之；如個人資料正確性發生爭議，即應停止處理或利用，以避免當事人遭受因資料不正確而生之損害，爰為第五款規定。
第十一條 非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。	為尊重當事人能知曉其個人資料被蒐集、處理及利用之狀況，本法第八條及第九條規定資料蒐集者有告知義務。非公務機關應區分個人資料蒐集方式為直接蒐集或間接蒐集，分別訂定告知之方式、內容及相關注意事項，以便所屬人員於辦理業務時能據以執行。
第十二條 中央主管機關依本法第二十一條規定，對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。 非公務機關將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督： 一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。 二、當事人行使本法第三條所定權利之相關事項。	第一項規定非公務機關如受本法第二十一條規定之命令或處分，應遵循之；第二項規定其進行個人資料國際傳輸前，應檢視有無本法第二十一條規定限制情形，並告知當事人欲傳輸個人資料之目的區域，且對資料接收方為適當監督。
第十三條 非公務機關於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理： 一、提供聯絡窗口及聯絡方式。 二、確認為個人資料當事人本人，或經其委託者。 三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。 四、有收取必要成本費用者，應告知當事人收費基準。 五、遵守本法第十三條有關處理期限	定明非公務機關於當事人行使本法第三條規定之權利時之應辦事項，如應設置聯絡窗口，採取相關方法協助當事人行使本法第三條、第十條及第十一條規定之權利，依本法第十三條規定於處理期限內為准駁決定，必要時得延長，並應將其原因以書面通知請求人。如有本法第十條及第十一條得拒絕當事人行使權利之事由，一併附理由通知當事人。另依本法第十四條規定，非公務機關對於查詢或請求閱覽個人資料或製給複製本者，得酌收必要成本費用。

之規定。	
第十四條 非公務機關為維護所保有個人資料之安全，使用存有個人資料之各類設備或儲存媒體，應採取下列資料安全管理措施： 一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定各類設備或儲存媒體之使用規範。 二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。 三、作業過程有備份個人資料之需要時，該備份資料比照原件，依本法規定予以保護之。 四、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，於報廢、汰換或轉作其他用途時，應採適當防範措施，以避免由該媒介物洩漏個人資料；委託他人執行者，非公務機關對受託人之監督依第二十二條規定辦理。	一、非公務機關應訂定各類設備或儲存媒體等之使用規範，以防範個人資料經各類設備或儲存媒體（如筆記型電腦、行動裝置、隨身碟）洩漏，爰為第一款規定。 二、使用各類設備或儲存媒體進行蒐集、處理或利用個人資料時，如有加密之需要，應採取適當之加密機制，例如隨身碟加密或電子檔案加密，爰為第二款規定。 三、使用存有個人資料之各類設備或儲存媒體，有備份個人資料之需要時，應比照原件保護備份檔案。原件所採取之相關個人資料安全維護措施，備份亦應比照原件辦理，個人資料備份應遵守本法規定採取適當保護措施，爰為第三款規定。 四、儲存個人資料之媒介物，進行個人資料之報廢、汰換或轉用作業，應採取適當措施防範個人資料經該媒介物洩漏；委託他人執行時，非公務機關應適當監督，爰為第四款規定，以下例示說明： （一）報廢作業：儲存個人資料之媒介物報廢時應進行銷毀，以確保資料無法再利用，以光碟為例，應將欲銷毀之光碟造冊列管，銷毀過程應有專人全程監看，確認已銷毀（例如燒毀、裁碎、消磁或破壞，且確認個人資料已無法被使用），應於文件簽名並留存紀錄備查。 （二）汰換或轉作他用作業：如隨身碟原用於儲存住戶管理資料，轉為存放建築藍圖用途，應確保個人資料已清空，於文件簽名並留存紀錄備查。
第十五條 非公務機關使用資通訊系統蒐集、處理或利用個人資料，且其資料庫保有個人資料數量達五千筆以上者，應採取下列措施： 一、使用者身分確認及保護機制。 二、個人資料顯示之隱碼機制。 三、網際網路傳輸之安全加密機制。 四、個人資料檔案與資料庫之存取控制及保護監控措施。	一、依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，並參酌製造業及技術服務業個人資料檔案安全維護管理辦法第二條規定，保有個人資料筆數達五千筆以上之業者，應針對非公務機關使用資通訊系統蒐集、處理或利用個人資料，加強管理措施，爰為第一項規定，其各款措施具體執行方式

五、防止外部網路入侵對策。 六、非法或異常使用行為之監控及因應機制。 前項第五款及第六款所定措施，應定期演練及檢討改善。	，可參考資通安全責任等級分級辦法附表十資通系統防護基準，例示如下： (一) 系統應建立帳號管理機制，包含帳號申請、建立、修改、啟用、停用及刪除程序，並執行身分驗證管理，如身分驗證資訊不以明文傳輸、密碼複雜度或帳號鎖定機制等。 (二) 系統界面呈現個人資料時，應以適當且一致性之隱碼或遮罩處理，以避免過多且非必要之個人資料揭露，可參考 CNS 二九一九一「資訊技術—安全技術—部分匿名及部分去連結鑑別之要求事項」國家標準。 (三) 個人資料傳輸時，應採用傳輸加密機制，如採用加密傳輸通道、使用公開、國際機構驗證且未遭破解之演算法。 (四) 儲存於電子媒體及資料庫之個人資料，應適當加密保護，並提供使用者識別、鑑別及身分管理，並採用最小權限原則進行存取控制管理。 (五) 針對外部入侵之防禦，應採用適當資安控制措施建立防禦縱深，包括防毒軟體、防火牆、入侵偵測與防禦系統及應用程式防火牆等。 (六) 針對系統或個人資料檔案之存取，應確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件，且應留存系統相關日誌紀錄並定期檢視，或設置適當監控及異常行為預警機制。 二、隨網路科技之進步，個人資料遭外部網路入侵、非法或異常使用行為損害情形層出不窮，爰第二項定明針對第一項第五款及第六款所定措施，非公務機關應定期進行演練及檢討改善。
第十六條 非公務機關對保有個人資料之環境及實體設備安全，應採取下列措施： 一、依據作業內容之不同，實施適宜之進出管制方式。 二、訂定媒介物之管制方式，並檢視其保管情形。 三、針對不同媒介物存在之環境，建	一、第一項第一款規定非公務機關應針對保有個人資料之環境及實體設備（例如檔案室、機房、大型設備或基礎設施），採取進出管制。 二、第一項第二款規定應建立第十四條第四款所定媒介物之保管方式及管制機制，例如人員交接應返還所保管之媒介物，檢視媒介物之使用去向。

置適度之保護設備或技術。 前項所稱環境，指第十四條所定各類設備、儲存媒體或媒介物之存放區域。	三、第一項第三款規定應針對不同媒介物存在之環境，採取適當監控及保護措施，例如：存放待報廢光碟之區域應避免他人接觸，以防範個人資料因環境外洩。 四、第二項定明第一項所稱環境之內涵。本辦法對硬體安全之保護規範有二，第十四條針對保有個人資料之小型設備及媒介物，由保管人保管，存放地點分散；本條針對保有個人資料之環境，保管人為部門或供應商，存放地點集中。
第十七條 非公務機關為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。 前項管理措施，應包括下列事項： 一、依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。 二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。 三、要求所屬人員妥善保管存有個人資料之媒介物，並約定保管及保密義務。 四、所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。	一、非公務機關及所屬人員，不論何種法律關係，業者都必須避免個人資料之保管及處理發生弊端，導致侵害當事人權益情事，爰第一項規定應於所訂計畫中，對所屬人員採取必要且適當之管理措施。 二、非公務機關應根據業務性質，檢視容易發生問題之處，預先予以防範。例如：與業務無關人員不得任意接觸資料、授予必要利用個人資料人員不同等級之權限、所屬人員在個人資料蒐集、處理及利用流程中有無漏洞、約束規範嚴密保管個人資料檔案及所屬人員異動或離職時，所持有之個人資料如何交接及保密切結等事項，爰為第二項規定。
第十八條 非公務機關應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍、各種個人資料保護事項之作業程序及應遵守之相關管理措施。	為提升非公務機關所屬人員個人資料保護及管理能力，非公務機關應定期或不定期辦理個人資料保護認知宣導及教育訓練。
第十九條 非公務機關為確保本計畫及處理方法之落實，應依其業務規模及特性，衡酌經營資源之合理分配，訂定個人資料安全維護稽核機制，並指定適當人員每半年至少進行一次本計畫及處理方法執行情形之檢查。 前項檢查結果應向負責人提出報告，並留存相關紀錄，其保存期限至	一、第一項及第二項規定非公務機關訂定之本計畫及處理方法應包含個人資料安全維護稽核機制，由適當人員檢查本計畫及處理方法是否落實執行，並應將檢查結果報告非公務機關負責人，且須留存相關紀錄至少五年。 二、第三項規定檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者

少五年。 非公務機關依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。	，非公務機關應作必要之改善。
第二十條 非公務機關執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。 非公務機關依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： 一、刪除、停止處理或利用之方法、時間或地點。 二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。 前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。	一、為確保個人資料檔案蒐集、處理或利用之合法正當，非公務機關應有證據保存機制，例如個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據等文件或檔案，以供說明其執行各個人資料保護事項之情況，爰為第一項規定。 二、保有及管理個人資料，如特定目的已消失或期限已屆滿，應依本法第十一條第三項規定予以刪除、停止處理或利用，爰為第二項規定 三、本法第三十條規定之損害賠償請求權時效為五年，爰於第三項規定，除法令另有規定或契約另有約定者外，第一項及第二項之軌跡資料、相關證據及紀錄之保存期限至少五年。
第二十一條 非公務機關應隨時參酌業務與本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定本計畫及處理方法，必要時予以修正；修正時，應於十五日內將修正後之本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。	由於科技發展不斷進步，社會活動型態亦隨時改變，爰定明非公務機關應注意媒體對個人資料侵害或保護事件相關報導，並配合個人資料保護法令之訂修，隨時檢討所定本計畫及處理方法。如有不合時宜之處，應立即修正，以落實保護個人資料。
第二十二條 非公務機關委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人依本法施行細則第八條規定為適當之監督。 非公務機關為執行前項監督，應與受託人明確約定相關監督事項及方式。	依本法施行細則第八條規定，非公務機關如將個人資料之蒐集、處理或利用委託他人為之，應對受託人為適當之監督，以使資料之蒐集、處理或利用仍符合法令之要求，爰為第一項規定，並於第二項規定非公務機關應與受託人約定相關監督事項及方式。
第二十三條 非公務機關業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。	非公務機關因解散、歇業、公司合併或其他原因終止業務後，自不得再繼續持有使用個人資料，應作妥善處置，爰定明終止業務之非公務機關，應視其終止業務之原因，將所保有之個人資料予以銷毀、移轉或其他刪除、停止處理或利用等方式處理。非公務機關在銷毀、移轉或其他刪除、停止處理或利用個人資料過程中，宜保存執行方法、時間、地點、執行人員、接受

三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。	移轉個人資料之對象及合法移轉個人資料之法規依據等資料，以便日後舉證。
第二十四條 本辦法發布施行前，未訂定本計畫及處理方法之非公務機關，應依本辦法規定訂定，並於本辦法發布施行日起六個月內，將本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。	本辦法施行前之非公務機關，應依本辦法訂定本計畫及處理方法，並於一定期間內報備查。
第二十五條 本辦法自發布日施行。	本辦法施行日期。

附件 個人資料事故通報及紀錄表

個人資料事故通報及紀錄表		
非公務機關名稱 _____	通報時間： 年 月 日 時 分 通報人： _____ 簽名(蓋章) 職稱： _____ 電話： _____ Email： _____ 地址： _____	
通報機關 _____		
發生時間		
發生種類	☐ 竊取 ☐ 竄改 ☐ 毀損 ☐ 滅失 ☐ 洩漏 ☐ 其他侵害情形	個人資料侵害之總筆數(大約)：_
		☐ 一般個人資料：_____ 筆 ☐ 特種個人資料：_____ 筆
發生原因及摘要		
損害狀況		
個人資料侵害可能結果		
擬採取之因應措施		
擬通知當事人之時間及方式		
是否於發現個人資料外洩後七十二小時內通報	☐ 是 ☐ 否，理由： _____	

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。

說明：配合第九條第一項規定之。